(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 333 376 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
06.03.2024 Bulletin 2024/10

(21) Application number: **21945014.5**

(22) Date of filing: **07.06.2021**

(51) International Patent Classification (IPC):
H04L 12/00 *(2006.01)*

(86) International application number:
PCT/JP2021/021635

(87) International publication number:
WO 2022/259335 (15.12.2022 Gazette 2022/50)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(71) Applicant: **Nippon Telegraph And Telephone Corporation
Chiyoda-ku
Tokyo 100-8116 (JP)**

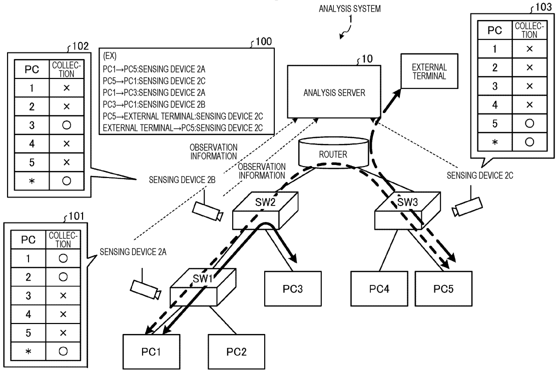
(72) Inventors:
- **TERAMOTO, Yasuhiro
Musashino-shi, Tokyo 180-8585 (JP)**
- **YAMADA, Masanori
Musashino-shi, Tokyo 180-8585 (JP)**
- **NAGAFUCHI, Yukio
Musashino-shi, Tokyo 180-8585 (JP)**
- **SHINOHARA, Masanori
Musashino-shi, Tokyo 180-8585 (JP)**
- **KOYAMA, Takaaki
Musashino-shi, Tokyo 180-8585 (JP)**
- **NAKAJIMA, Yoshiaki
Musashino-shi, Tokyo 180-8585 (JP)**

(74) Representative: **Hoffmann Eitle
Patent- und Rechtsanwälte PartmbB
Arabellastraße 30
81925 München (DE)**

(54) ANALYSIS DEVICE, ANALYSIS METHOD, AND ANALYSIS PROGRAM

(57) An analysis server (10) acquires observation information including a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address in communication from each of sensing devices (2). The analysis server (10) estimates a topology of a network on the basis of the acquired observation information. On the basis of the estimated topology, an analysis server (10) creates a monitoring list indicating communication that is a target for transmission of the observation information for each sensing device (2) such that any one sensing device (2) on a path of the communication transmits the observation information of the communication for each piece of communication in the network, and transmits the monitoring list to the sensing device (2). Thereafter, each sensing device (2) transmits the observation information of the communication to the analysis server (10) on the basis of the monitoring list.

Fig. 1



(EX)
PC1→PC5:SENSING DEVICE 2A
PC5→PC1:SENSING DEVICE 2C
PC1→PC3:SENSING DEVICE 2A
PC3→PC1:SENSING DEVICE 2B
PC5→EXTERNAL TERMINAL:SENSING DEVICE 2C
EXTERNAL TERMINAL→PC5:SENSING DEVICE 2C

PC	COLLECTION
1	×
2	×
3	○
4	×
5	×
*	○

PC	COLLECTION
1	○
2	○
3	×
4	×
5	×
*	○

PC	COLLECTION
1	×
2	×
3	×
4	×
5	○
*	○

Processed by Luminess, 75001 PARIS (FR)

Description

Technical Field

[0001] The present invention relates to an analysis apparatus, an analysis method, and an analysis program for analyzing communication in a network.

Background Art

[0002] Conventionally, there is a technology in which, in order to monitor communication in a network without omission, communication in the network is observed by a plurality of sensing devices and observation information is acquired. The observation information is information indicating an observation result of communication, and includes IP addresses of a transmission source and a transmission destination, MAC addresses of the transmission source and the transmission destination, and the like of the communication.

Citation List

Patent Literature

[0003] Patent Literature 1: Japanese Patent No. 4809880

Summary of Invention

Technical Problem

[0004] However, when communication in a network is observed by a plurality of sensing devices, the same communication may be observed by the plurality of sensing devices. In such a case, an analysis server redundantly receives observation information of the same communication from a plurality of sensing devices, and thus reception efficiency of the observation information is not good.

[0005] In a case where a plurality of sensing devices observe communication across a plurality of Layer 3 networks (L3 NWs), different MAC addresses are set for an interface of a router installed at a boundary between the networks. Therefore, the analysis server may receive observation information with different MAC addresses associated with IP addresses from a plurality of sensing devices.

[0006] In such a case, the analysis server cannot determine whether the MAC addresses associated with the IP addresses are different due to routing or impersonation of a terminal. Thus, when the analysis server performs detection of an impersonated terminal or the like by using a pair of an IP address and a MAC address indicated in observation information of communication, there is a possibility of erroneous detection.

[0007] Therefore, an object of the present invention is to solve the above problem and appropriately monitor communication in a network.

Solution to Problem

[0008] In order to solve the above problems, the present invention provides an analysis apparatus including: an acquisition unit that acquires observation information of communication including a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address in the communication from each communication observation device that observes the communication in a network; an estimation unit that estimates a topology of the network on the basis of the acquired observation information; an allocation unit that allocates the communication observation devices such that any one communication observation device on a path of the communication transmits the observation information of the communication for each piece of communication flowing through the network on the basis of the estimated topology, an installation position of the communication observation device, and the observation information of the communication acquired from the communication observation device; a list creation unit that creates a monitoring list indicating communication that is a target for transmission of the observation information from the communication observation device for each communication observation device on the basis of a result of the allocation, and a list transmission unit that transmits the created monitoring list for each of the communication observation devices to each of the communication observation devices.

Advantageous Effects of Invention

[0009] According to the present invention, it is possible to appropriately monitor communication in a network.

Brief Description of Drawings

[0010]

Fig. 1 is a diagram for describing an outline of an analysis system.
Fig. 2 is a diagram illustrating a configuration example of the analysis system.
Fig. 3 is a diagram for describing a monitoring list.
Fig. 4 is a diagram for describing estimation 1 of a MAC address of a router.
Fig. 5 is a diagram for describing estimation 2 of a MAC address of a router and estimation of an IP address of an external terminal.
Fig. 6 is a diagram for describing estimation of a topology.
Fig. 7 is a sequence diagram illustrating an example of a processing procedure of the analysis system.
Fig. 8 is a flowchart illustrating details of processes in S13 and S14 in Fig. 7.

Fig. 9 is a diagram for describing estimation of an L2 topology performed by the analysis server.

Fig. 10 is a diagram for describing estimation of a topology of a network in which routers are hierarchically installed, performed by the analysis server.

Fig. 11 is a diagram illustrating an example of a network configured by a white box switch (WB SW) having a function of a sensing device.

Fig. 12 is a diagram illustrating a configuration example of a computer that executes an analysis program.

Description of Embodiments

[0011] Hereinafter, modes for carrying out the present invention (embodiments) will be described with reference to the drawings. The present invention is not limited to the embodiments described below.

[Outline]

[0012] First, an outline of an operation of an analysis system 1 including an analysis apparatus (analysis server) 10 will be described with reference to Fig. 1. The analysis system 1 includes sensing devices 2 (for example, sensing devices 2A, 2B, and 2C) and an analysis server 10. Switching hubs (SWs; for example, SW1, SW2, and SW3) are installed in a network.

[0013] Each sensing device (communication observation device) 2 observes communication in the network that is a monitoring target. For example, each sensing device 2 observes communication between PCs (terminals) via the SW in the network that is a monitoring target by using a port mirror or the like, and creates observation information. Each sensing device 2 transmits the created observation information to the analysis server 10. The observation information includes, for example, a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address of communication in an observation target.

[0014] The analysis server 10 estimates a topology (refer to Fig. 1) of the network that is a monitoring target on the basis of the observation information received from each sensing device 2. The analysis server 10 creates, for each sensing device 2, a monitoring list indicating communication that is a target for transmission (collection target) of the observation information from the sensing device 2, on the basis of the estimated topology.

[0015] For example, on the basis of the estimated topology, the analysis server 10 allocates the sensing devices 2A, 2B, and 2C such that any one of the sensing devices 2 on a path of communication transmits observation information of the communication for each piece of communication flowing in the network (refer to the reference numeral 100).

[0016] The analysis server 10 creates, for each sensing device 2, for example, a monitoring list (for example, monitoring lists 101, 102, and 103) indicating communication that is a target for transmission of the observation information from the sensing device 2 on the basis of an allocation result denoted by the reference numeral 100. The analysis server 10 transmits the created monitoring lists to the sensing devices 2A, 2B, and 2C.

[0017] For example, the analysis server 10 transmits the monitoring list 101 to the sensing device 2A, transmits the monitoring list 102 to the sensing device 2B, and transmits the monitoring list 103 to the sensing device 2C. Each of the sensing devices 2A, 2B, and 2C transmits observation information of communication to the analysis server 10 on the basis of the monitoring list transmitted from the analysis server 10.

[0018] For example, in the communication illustrated in Fig. 1, the sensing device 2A transmits observation information of communication from PC1 to PC5 and communication from PC1 to PC3 to the analysis server 10 on the basis of the monitoring list 101. The sensing device 2B transmits observation information of communication from PC3 to PC1 to the analysis server 10 on the basis of the monitoring list 102. The sensing device 2C transmits observation information of communication from PC5 to an external terminal and from the external terminal to PC5 to the analysis server 10 on the basis of the monitoring list 103.

[0019] As described above, the analysis server 10 can prevent observation information of the same communication from being redundantly received from each sensing device 2 as far as possible.

[0020] The analysis server 10 can estimate an IP address and a MAC address of a router in a network and an IP address of a terminal (external terminal) installed outside the network (that is, the outside of the network divided by the router) on the basis of the observation information received from each of the sensing devices 2. As a result, the analysis server 10 can reduce erroneous detection in detection of an impersonated terminal by using the IP address and MAC address indicated in the observation information from each sensing device 2.

[0021] The analysis server 10 transmits, for each sensing device 2, a monitoring list indicating communication that is to be a target for transmission of observation information from the sensing device 2 to the sensing device 2. Consequently, each sensing device 2 can determine which observation information is to be transmitted without making an inquiry to another device.

[Configuration example]

[0022] Next, a configuration example of the analysis system 1 will be described with reference to Fig. 2. The analysis system 1 includes the plurality of sensing devices 2 and the analysis server 10.

[0023] The sensing device 2 transmits, to the analysis server 10, observation information of communication indicated in the monitoring list (refer to the monitoring lists 101 to 103 in Fig. 1) transmitted from the analysis server

10.

[0024] The analysis server 10 includes a communication unit 11, a storage unit 12, and a control unit 13. The communication unit 11 is a communication interface with an external device. The communication unit 11 receives observation information from the sensing device 2 or transmits a monitoring list to the sensing device 2 via a network such as the Internet.

[0025] The storage unit 12 stores data to be referred to when the control unit 13 executes various processes and data created by the control unit 13 executing various processes. For example, the storage unit 12 stores observation information acquired from each of the sensing devices 2 or information (topology information) indicating a topology of a network created by the control unit 13.

[0026] The control unit 13 controls the entire analysis server 10. The control unit 13 includes an acquisition unit 130, an estimation unit 131, an allocation unit 132, a list creation unit 133, a list transmission unit 134, an analysis unit 135, and a control processing unit 136.

[0027] The acquisition unit 130 acquires observation information of communication from each sensing device 2. The acquisition unit 130 stores the acquired observation information in the storage unit 12.

[0028] The estimation unit 131 estimates a topology of the network on the basis of the observation information acquired from each sensing device 2. That is, the estimation unit 131 estimates a disposition and connection of a router, an apparatus (for example, a SW), and a terminal (for example, a PC) of the network that is a monitoring target, and an IP address and a MAC address allocated to each device. The estimation unit 131 estimates a router via which an external terminal of the network that is a monitoring target is connected and an IP address allocated to the external terminal.

[0029] For example, the estimation unit 131 estimates an IP address and a MAC address of the terminal, an IP address and a MAC address of the router, and an IP address of the external terminal of the network that is a monitoring target, on the basis of a difference between pieces of observation information acquired from the respective sensing devices 2. The estimation unit 131 estimates a topology (for example, the topology illustrated in Fig. 1) of an L2 network in a subnet by using the estimation result. Details of estimation of a topology by the estimation unit 131 will be described later with reference to the drawings.

[0030] The allocation unit 132 allocates communication that is a target for transmission of observation information from each sensing device 2 on the basis of the topology estimated by the estimation unit 131, the installation position of each sensing device 2, and the observation information of communication from each sensing device 2.

[0031] For example, the allocation unit 132 allocates each sensing device 2 for each piece of communication flowing through the network such that any one of the sensing devices 2 of SWs on a path of the communication transmits the observation information of the communication on the basis of the topology estimated by the estimation unit 131, the installation position of each sensing device 2, and the observation information of the communication from each sensing device 2.

[0032] For example, the allocation unit 132 allocates the sensing device 2A as the sensing device 2 that transmits observation information of communication from PC1 to PC5 among the sensing devices 2 (2A, 2B, and 2C) of SW1, SW2, and SW3 on the path from PC1 to PC5 illustrated in Fig. 1. The list creation unit 133 allocates the sensing device 2C as the sensing device 2 that transmits observation information of communication from PC5 to PC1 among the sensing devices 2 (2A, 2B, and 2C) of SW1, SW2, and SW3 on the path from PC5 to PC1.

[0033] The allocation unit 132 performs the above allocation process on the sensing device 2 for each piece of communication flowing through the network. Consequently, communication that is to be a target for transmission of observation information is allocated to each sensing device 2.

[0034] The list creation unit 133 creates a monitoring list indicating communication that is a target for transmission of observation information for each sensing device 2 on the basis of the allocation result from the allocation unit 132. For example, as illustrated in the monitoring lists 101 to 103 in Fig. 1, this monitoring list is information indicating a transmission source IP address related to communication that is a target for transmission of the observation information from the sensing device 2 and a transmission source IP address related to communication that is not a target for transmission.

[0035] The monitoring list will be described in detail with reference to Fig. 3. Here, a case is considered in which the list creation unit 133 creates a monitoring list 301 for the sensing device 2A and a monitoring list 302 for the sensing device 2B illustrated in Fig. 3, and creates a monitoring list 303 for the sensing device 2C.

[0036] For example, the monitoring list 301 indicates that communication in which transmission sources are PC1 and PC2 is a target for transmission of observation information, but communication in which transmission sources are PC3, PC4, and PC5 is not a target for transmission of observation information. It is indicated that all pieces of communication in which transmission sources are not PC3, PC4, and PC5 are targets for transmission of observation information.

[0037] The monitoring list 302 indicates that communication in which transmission sources are PC3 and PC4 is a target for transmission of observation information, but communication in which transmission sources are PC1, PC2, and PC5 is not a target for transmission of observation information. It is indicated that all pieces of communication in which transmission sources are not PC1, PC2, and PC5 are targets for transmission of observation information.

[0038] The monitoring list 303 indicates that communication in which a transmission source is PC5 is a target for transmission of observation information, but communication in which transmission sources are PC1, PC2, PC3, and PC4 is not a target for transmission of observation information. It is indicated that all pieces of communication in which transmission sources are not PC1, PC2, PC3, and PC4 are targets for transmission of observation information.

[0039] For example, the sensing device 2A transmits observation information of communication from PC1 to PC3 to the analysis server 10 but does not transmit observation information of communication from PC3 to PC1 to the analysis server 10 on the basis of the monitoring list 301.

[0040] The sensing device 2B transmits observation information of communication from PC3 to PC1 to the analysis server 10 but does not transmit observation information of communication from PC1 to PC3 to the analysis server 10 on the basis of the monitoring list 302.

[0041] The sensing device 2C transmits observation information of communication from W2 (external terminal) to PC5 and observation information of communication from PC5 to W2 to the analysis server 10 on the basis of the monitoring list 303.

[0042] Consequently, the analysis server 10 can reduce a possibility of redundantly receiving observation information of the same communication from each sensing device 2. For example, in a case where there is only one sensing device 2 on the communication path as in the communication between W2 and PC5 illustrated in Fig. 3, the analysis server 10 creates the monitoring list 303 in which the sensing device 2 (that is, the sensing device 2C) transmits observation information of the communication from W2 to PC5 and the communication from PC5 to W2, and transmits the monitoring list to the sensing device 2C. Consequently, the analysis server 10 can receive observation information of communication in the network that is a monitoring target without omission.

[0043] The description returns to Fig. 2. The list transmission unit 134 transmits the monitoring list created by the list creation unit 133 to each sensing device 2. For example, the list transmission unit 134 transmits the monitoring list 301 illustrated in Fig. 3 to the sensing device 2A, transmits the monitoring list 302 to the sensing device 2B, and transmits the monitoring list 303 to the sensing device 2C.

[0044] The description returns to Fig. 2. The analysis unit 135 analyzes communication in the network on the basis of the observation information of each piece of communication in the network acquired by the acquisition unit 130.

[0045] For example, when the observation information is acquired via the acquisition unit 130, the analysis unit 135 detects communication performed by an impersonated terminal by comparing a pair of the transmission source IP address and the transmission source MAC address in the observation information with a pair of an IP address and a MAC address of each terminal, router, or the like indicated in the topology information stored in the storage unit 12.

[0046] For example, the analysis unit 135 detects a change in the topology on the basis of the observation information of the communication acquired by the acquisition unit 130. For example, the analysis unit 135 detects the presence or absence of a change in the topology by comparing an estimated new topology with the topology stored in the storage unit 12 on the basis of the observation information acquired by the acquisition unit 130. When it is detected that there is a change in the topology, the analysis unit 135 outputs a detection result (for example, which terminal in the network has been added and which terminal has been moved).

[0047] Consequently, a user of the analysis server 10 can ascertain that there is a possibility that an unauthorized terminal has been connected to the network and that there has been a change in the network configuration due to movement of a terminal or an apparatus.

[0048] The control processing unit 136 controls each unit of the control unit 13. For example, in a case where the analysis unit 135 detects that there is a change in the topology of the network, when the user of the analysis server 10 determines that the change in the topology is not illegal, the control processing unit 136 instructs the allocation unit 132 to allocate communication that is a target for transmission of observation information from each sensing device 2 on the basis of the estimated new topology and the observation information.

[0049] In response to the instruction, the list creation unit 133 reallocates communication that is a target for transmission of observation information from each sensing device 2 on the basis of the estimated new topology and the observation information. Next, the list creation unit 133 recreates the monitoring list for each of the sensing devices 2 by using the result of the reallocation described above. Thereafter, the list transmission unit 134 transmits the recreated monitoring list to each sensing device 2. Thereafter, each sensing device 2 transmits observation information on the basis of the new monitoring list.

[0050] Consequently, the analysis server 10 can appropriately receive observation information from each of the sensing devices 2 even when there is a change in a network configuration.

[Processing example]

[0051] Next, estimation of a topology of a network by the estimation unit 131 and creation of a monitoring list by the list creation unit 133 will be described with reference to Figs. 4 to 6.

(Estimation 1 of MAC address of router)

[0052] First, estimation of an IP address of a router and a MAC address associated with the IP address by the estimation unit 131 will be described with reference to Fig. 4.

[0053] Here, a case where the sensing device 2 acquires observation information from SW1, SW2, and SW3 in a network denoted by the reference numeral 401 will be described as an example. An arrow denoted by the reference numeral 401 indicates communication in the network. In the network denoted by the reference numeral 401, W1 and W2 denote external terminals, and RT denotes a router.

[0054] The estimation unit 131 creates a list 402 indicating observation information of communication (a transmission source IP address (Src IP), a transmission source MAC address (Src MAC), a transmission destination IP address (Dst IP), and a transmission destination MAC address (Dst MAC) of the communication) via SW1, SW2, and SW3 acquired by the acquisition unit 130. The estimation unit 131 creates, for each MAC address, the list 403 indicating an IP address associated with the MAC address on the basis of the list 402.

[0055] Here, the router replaces a MAC address of an IP address of a packet that is a routing target with a MAC address allocated to the router. Therefore, a plurality of IP addresses are associated with the MAC address allocated to the router. Thus, in the list 403, the MAC address of the router is associated with a plurality of IP addresses. Therefore, the estimation unit 131 estimates R1 and R2, which are MAC addresses associated with a plurality of IP addresses in the list 403, as MAC addresses of the router.

(Estimation 2 of MAC address of router)

[0056] Fig. 5 will be described. Next, for each pair of (a transmission source IP address (Src IP) and a transmission destination IP address (Dst IP)) in the list 402, the estimation unit 131 creates a list 501 indicating a pair of (a transmission source MAC address (Src MAC) and a transmission destination MAC address (Dst MAC)) corresponding to the pair.

[0057] Here, in the list 501, when there are a plurality of (a transmission source MAC address, a transmission destination MAC address) pairs for the same (transmission source IP address and transmission destination IP address) and a transmission destination MAC address in one of the pairs is the MAC address of the router estimated in (Estimation 1 of MAC address of router) described in Fig. 4, the transmission source MAC addresses of the other pairs can be considered as a MAC address of an exit IF (interface) of the router (refer to the reference numeral 502).

[0058] For example, pairs of (transmission source MAC address, transmission destination MAC address) for (PC1, PC5) in the list 501 are (PC1, R1) and (R3, PC5). Of the pairs, the transmission destination MAC address (R1) in the pair of (PC1, R1) is a MAC address of the router estimated in (Estimation 1 of MAC address of router) described in Fig. 4.

[0059] Here, the transmission source MAC address (R3) in another pair (R3, PC5) is not estimated as a MAC address of the router in (Estimation 1 of MAC address of router) described in Fig. 4, but can be considered as a MAC address of the exit IF of the router (refer to the reference numeral 502).

[0060] Therefore, the estimation unit 131 estimates R3 in the above pair of (R3, PC5) as the MAC address of the router (refer to (1) in the list 501). By performing the above process, the estimation unit 131 can also estimate the MAC address of the router that cannot be estimated in (Estimation 1 of MAC address of router) described with reference to Fig. 4.

(Estimation of external terminal)

[0061] In the list 501 illustrated in Fig. 5, in a case where there is only one pair of (transmission source MAC address, transmission destination MAC address) with respect to the same (transmission source IP address, transmission destination IP address), and it is ascertained that a transmission destination MAC address in the pair is the MAC address of the router, the pair of (transmission source IP address, transmission destination IP address) can be considered to be a pair with an IP address of the external terminal (refer to the reference numeral 502 and (2) in the list 501).

[0062] Therefore, for example, each of the pairs of IP addresses of (PC1, W1) and (PC1, W2) in the list 501 can be considered as a pair indicating communication with the external terminal. Therefore, the estimation unit 131 estimates W1 and W2 as IP addresses of the external terminals.

(Estimation of topology)

[0063] Next, estimation of a topology of a network by the estimation unit 131 will be described with reference to Fig. 6. The estimation unit 131 estimates a topology of the network by using the MAC address of the router and the IP address of the external terminal estimated through the above process.

[0064] For example, the estimation unit 131 estimates the topology of the network indicated by the reference numeral 602 by using observation information (transmission source IP addresses (Src IP), transmission source MAC addresses (Src MAC), transmission destination IP addresses (Dst IP), and transmission destination MAC addresses (Dst MAC) of communication) of SW1, SW2, and SW3 denoted by the reference numeral 601 in Fig. 6 and the MAC address of the router and the IP address of the external terminal estimated through the above process.

[0065] On the basis of the estimated topology, the allocation unit 132 performs allocation for each piece of communication flowing through the network such that any one of the sensing devices 2 capable of transmitting observation information of the communication transmits the observation information of the communication.

[0066] For example, in the topology denoted by the reference numeral 601, the allocation unit 132 allocates communication of PC1 and PC2 to the sensing device 2 of SW1, allocates communication of PC3 and PC4 to the sensing device 2 of SW2, and allocates communication of PC5 to the sensing device 2 of SW3.

[0067] The list creation unit 133 creates monitoring lists 603 to 605 on the basis of the allocation results. That is, the list creation unit 133 creates the monitoring list 603 for the sensing devices 2 of SW1, creates the monitoring list 604 for the sensing devices 2 of SW2, and creates the monitoring list 605 for the sensing devices 2 of SW3. Thereafter, the list transmission unit 134 transmits the monitoring lists 603 to 605 to the target sensing devices 2. Each sensing device 2 transmits observation information of communication indicated in the received monitoring list to the analysis server 10.

[0068] As described above, the analysis server 10 can appropriately receive observation information of communication in the network from each sensing device 2.

[Example of processing procedure]

[0069] Next, an example of a processing procedure of the analysis system 1 will be described with reference to Fig. 7. First, the acquisition unit 130 of the analysis server 10 transmits an instruction for transmitting observation information of communication to each sensing device 2 (S1). Each of the sensing devices 2 creates observation information of communication via the SW in the network that is a monitoring target on the basis of the above instruction, and transmits the observation information to the analysis server 10 (S2).

[0070] Thereafter, the estimation unit 131 of the analysis server 10 creates a list of communication observed by the SW (refer to, for example, the list 402 in Fig. 4) for each apparatus (for example, the SW) in the network that is a monitoring target on the basis of the observation information of communication transmitted from each sensing device 2.

[0071] On the basis of the created list, the estimation unit 131 estimates a MAC address of the router in the network that is a monitoring target according to the method described in above (Estimation 1 of MAC address of router) (S3: Router Estimation 1). The estimation unit 131 estimates the MAC address of the router according to the method described in above (Estimation 2 of MAC address of router) (S4: Router Estimation 2). Consequently, the estimation unit 131 can also estimate the MAC address of the router that cannot be estimated in S3.

[0072] The estimation unit 131 estimates an IP address of the external terminal according to the method described in the above (Estimation of external terminal) on the basis of the created list (S5: Estimation of external terminal). The estimation unit 131 records an estimation result of the MAC address of the router and an estimation result of the IP address of the external terminal obtained through the above process in the above list (refer to the list 601 in Fig. 6).

[0073] After S5, in a case where the list has been updated (for example, update of the estimation result of the MAC address of the router or update of the estimation result of the IP address of the external terminal) in the above list through the processes up to S5 (Yes in S6), the estimation unit 131 executes the processes in and after S4 again.

[0074] On the other hand, in a case where there is no update (for example, update of the estimation result of the MAC address of the router or update of the estimation result of the IP address of the external terminal) in the above list through the processes up to S5 (No in S6), the estimation unit 131 estimates a topology of the network on the basis of the above list (S7).

[0075] After S7, the allocation unit 132 allocates communication that is a target for transmission of the observation information from each sensing device 2 on the basis of the estimation result of the topology in S7. The list creation unit 133 creates a monitoring list for each sensing device 2 on the basis of the allocation result (S8). Thereafter, the list transmission unit 134 transmits the monitoring list for each sensing device 2 to each sensing device 2.

[0076] Thereafter, each sensing device 2 starts monitoring communication on the basis of the transmitted monitoring list (S9). If the observed communication is a target for transmission of the observation information indicated in the monitoring list (Yes in S10), each sensing device 2 transmits the observation information of the communication to the analysis server 10. On the other hand, if the observed communication is not a target for transmission (No in S10), each sensing device 2 continues monitoring (S11), and returns to S10.

[0077] Thereafter, when the acquisition unit 130 of the analysis server 10 receives the observation information from the sensing device 2 (S12), the analysis unit 135 specifies an apparatus (for example, a PC) included in the observation information from the estimation result of the topology (topology information) in S7 (S13). The analysis unit 135 performs a communication abnormality detection process by using information regarding the apparatus specified in S13 (S14). The analysis unit 135 executes the processes in the above S13 and S14 each time the observation information is received from the sensing device 2.

[0078] The processes in S13 and S14 in Fig. 7 will be described in detail with reference to Fig. 8. For example, the analysis unit 135 specifies an apparatus ID and a current installation location (NW configuration) of each apparatus from a device ID of the sensing device 2, an apparatus IP (an IP address of the apparatus), and an apparatus MAC (a MAC address of the apparatus) indicated in the observation information received in S12 in Fig. 7 (S131 in Fig. 8).

[0079] The analysis unit 135 determines whether there is a difference between the NW configuration specified in S131 and the topology information stored in the storage unit 12 (S132).

[0080] Here, in a case where the analysis unit 135 determines that there is no difference between the NW configuration specified in S131 and the topology information stored in the storage unit 12 (No in S132), the process proceeds to S141. S141 will be described later.

[0081] On the other hand, in a case where the analysis unit 135 determines that there is a difference between the NW configuration specified in S131 and the topology information stored in the storage unit 12 (Yes in S132), information regarding the difference is output via the communication unit 11 (S133). Consequently, the user of the analysis server 10 can ascertain that the configuration of the network that is a monitoring target has been changed. Thereafter, the analysis server 10 receives input of a determination result regarding whether the configuration change of the network is a normal configuration change from the user. Here, in a case where the analysis unit 135 receives an input indicating that the configuration change of the network is a normal configuration change from the user (Yes in S134), the topology information is updated on the basis of the NW configuration specified in S131 (S135).

[0082] Thereafter, the analysis unit 135 performs a process of detecting communication details on the basis of the topology information updated in S135 and the observation information received in S12 in Fig. 7 (S141). For example, in a case where the pair of the IP address and the MAC address of the terminal indicated in the observation information received in S12 in Fig. 7 does not match the pair of the IP address and the MAC address indicated in the topology information, the analysis unit 135 detects the communication indicated in the observation information as communication performed by an impersonated terminal.

[0083] In a case where the analysis unit 135 detects an abnormality (for example, communication performed by an impersonated terminal) in the communication details through the detection process in S141 (Yes in S142), a notification indicating that the abnormality has been detected is sent through the communication unit 11 (S143: abnormality detection notification). Thereafter, the user handles the abnormality in the network on the basis of the notification.

[0084] On the other hand, in a case where analysis unit 135 does not detect an abnormality of the communication details through the detection process in S141 (No in S142), and when the topology information has been updated in S135 (Yes in S151), the process proceeds to S8 in Fig. 7. That is, on the basis of the topology information updated in S135, the allocation unit 132 reallocates communication that is a target for transmission of the observation information from each sensing device 2. The list creation unit 133 recreates a monitoring list for each of the sensing devices 2 on the basis of the reallocation result (S8 in Fig. 7). Thereafter, the list transmission unit 134 transmits the recreated monitoring list to each sensing device 2.

[0085] On the other hand, if the topology information has not been updated in S135 (No in S151 in Fig. 8), the process returns to S12 in Fig. 7. That is, the analysis server 10 waits for arrival of the observation information from the sensing device 2.

[0086] The analysis unit 135 outputs information regarding a difference between the NW configuration specified in S131 in Fig. 8 and the topology information stored in the storage unit 12 (S133), and in a case where it is determined by the user that some kind of abnormality has occurred in the configuration change of the network (No in S134), the user handles the abnormality in the network.

[0087] According to such an analysis server 10, each sensing device 2 is allocated such that the sensing device 2 of any one SW on a path of communication transmits observation information of the communication by using the estimated topology. Consequently, the analysis server 10 can reduce redundant transmission of the observation information from each sensing device 2.

[0088] For example, in a case where there is only one sensing device 2 capable of transmitting observation information of communication as in the communication between W2 and PC5 in Fig. 3 described above, the sensing device 2 transmits observation information of the communication to the analysis server 10. That is, the sensing device 2C in Fig. 3 transmits observation information for W2 to PC5 and observation information for PC5 to W2 to the analysis server 10. Consequently, the analysis server 10 can receive observation information of communication in the network that is a monitoring target without omission.

[0089] For example, as illustrated in Fig. 9, in a case where a plurality of SWs (SW1, SW2, and SW3) are installed in the same subnet and the sensing device 2 is installed in each of the SWs, the analysis server 10 can estimate an L2 topology by comparing observation information from each of the sensing devices 2 (sensing devices 2A, 2B, and 2C). For example, the analysis server 10 can estimate the L2 topology by comparing observation information according to the methods described in (Estimation 1 of MAC address of router) and (Estimation 2 of MAC address of router).

[0090] The analysis server 10 can estimate an IP address and a MAC address of the router and an IP address of the external terminal by comparing observation information according to the methods described in (Estimation 1 of MAC address of router) and (Estimation 2 of MAC address of router). As a result, when the analysis server 10 detects an impersonated terminal by using the IP address and the MAC address indicated in the observation information from each sensing device 2, it is possible to reduce erroneous detection.

[0091] According to the analysis server 10, for example, as illustrated in Fig. 10, even in a case where routers (RT1, RT2) are hierarchically installed and the sensing device 2 is not installed under any router (RT2), a topology can be estimated by the same algorithm as described above.

[0092] For example, PC1 and PC2 illustrated in Fig. 10 are terminals of a network different from the network to which SW1 belongs, but the sensing device 2A of SW1 always observes communication in which PC1 and PC2 are transmission sources or transmission destinations. From this, the analysis server 10 estimates that PC1 and PC2 are under control of SW1. The analysis server 10 estimates, for example, the topology illustrated in Fig. 10 as a topology of the network.

[0093] Thereafter, the analysis server 10 creates a monitoring list denoted by the reference numeral 1001 as a monitoring list for the sensing device 2A of SW1, for example, by using the estimation result of the topology. The analysis server 10 creates, for example, a monitoring list denoted by the reference numeral 1002 as a monitoring list for the sensing device 2B of SW2. The analysis server 10 acquires observation information transmitted from the sensing devices 2A and 2B on the basis of the monitoring list. Thus, the analysis server 10 can acquire observation information of communication between PC1 and PC2.

[0094] As described above, the analysis server 10 can also monitor communication between terminals in a complicated network such as a network in which routers are hierarchically installed as illustrated in Fig. 10. In a technique in which only a local network is a monitoring target as in the conventional technique, communication of terminals outside the local network, such as PC1 and PC2 in Fig. 10, cannot be monitored However, according to the analysis server 10 of the present embodiment, communication of terminals outside the local network, such as PC1 and PC2 in Fig. 10, can be monitored.

[0095] The analysis unit 135 of the analysis server 10 may output information regarding a monitoring location insufficient for monitoring communication in the network on the basis of the estimated topology of the network and the information regarding the installation location of the sensing device 2 in the network.

[0096] For example, in the network illustrated in Fig. 10, since observation information of the communication between PC1 and PC2 cannot be acquired with the current configuration, the analysis unit 135 recommends installing a new sensing device 2 at a location (for example, RT2) where the communication between PC1 and PC2 can be monitored. Consequently, the user of the analysis server 10 can ascertain a location where the sensing device 2 is added in order to monitor each piece of communication in the network without omission.

[0097] According to the analysis server 10, it is possible to estimate a topology that does not contradict an actual network configuration on the basis of the observation information transmitted from each sensing device 2. For example, there is a possibility that there is a location that the analysis server 10 cannot accurately estimate a network configuration depending on a case where observation information is insufficient or an installation location of the sensing device 2, but sensing (acquisition of observation information of communication from each sensing device 2) can be performed without any problem.

[0098] Even if estimation of a topology by the analysis server 10 is incomplete due to the lack of information, at least one sensing device 2 transmits observation information of each piece of communication, and thus missing of the observation information does not occur.

[0099] Since the analysis server 10 can detect new observation information or a network configuration change, connection of an unauthorized apparatus or movement of an apparatus can be detected. After detecting the configuration change of the network, the analysis server 10 can update the topology information and perform a communication detection process on the basis of the updated topology information and the observation information of the communication (refer to S141 in Fig. 7). Consequently, the analysis server 10 can appropriately perform a communication detection process.

[0100] After detecting the configuration change of the network, the analysis server 10 can recreate and transmit the monitoring list for each sensing device 2 on the basis of the updated topology information. Consequently, the analysis server 10 can appropriately receive observation information from each sensing device 2.

[0101] The network that is a monitoring target of the analysis server 10 may be a network configured by a white box switch (WB SW) having the function of the sensing device 2 (Fig. 11). In this case, the analysis server 10 transmits a monitoring list to each WB SW. Each WB SW transmits observation information of communication to the analysis server 10 on the basis of the monitoring list transmitted from the analysis server 10. The analysis server 10 monitors the communication in the network on the basis of the observation information of the communication transmitted from each WB SW.

[System configuration and the like]

[0102] Each constituent of each unit illustrated in the drawings is functionally conceptual and does not necessarily need to be physically configured as illustrated in the drawings. In other words, a specific form of distribution and integration of individual devices is not limited to the illustrated form, and all or some of the devices may be functionally or physically distributed and integrated in any unit according to various loads, usage conditions, and the like. All or some of the processing functions performed in the respective devices may be realized by a CPU and a program to be executed by the CPU or may be realized as hardware by wired logic.

[0103] Among the processes described in the above embodiment, all or some of the processes described as being automatically performed may be manually performed, or all or some of the processes described as being manually performed may be automatically performed according to a known method. The processing procedure, the control procedure, the specific name, and the information including various types of data and parameters that are illustrated in the document and the drawings can be freely changed unless otherwise specified.

[Program]

[0104] The analysis server 10 can be implemented by installing a program as package software or online software in a desired computer. For example, by causing an information processing apparatus to execute the above program, the information processing apparatus can be caused to function as the analysis server 10. The information processing apparatus mentioned here includes a desktop or a laptop personal computer. The information processing apparatus also includes a mobile communication terminal such as a smartphone, a mobile phone, or a personal handy-phone system (PHS) and a terminal such as a personal digital assistant (PDA).

[0105] The analysis server 10 may also be implemented as a server apparatus that uses a terminal apparatus used by a user as a client and provides the client with a service related to the above process. In this case, the server apparatus may be implemented as a web server or may be implemented as a cloud that provides a service related to the above process by outsourcing.

[0106] Fig. 12 illustrates an example of a computer that executes an analysis program. A computer 1000 includes, for example, a memory 1010 and a CPU 1020. The computer 1000 also includes a hard disk drive interface 1030, a disk drive interface 1040, a serial port interface 1050, a video adapter 1060, and a network interface 1070. These units are connected to each other via a bus 1080.

[0107] The memory 1010 includes a read only memory (ROM) 1011 and a random access memory (RAM) 1012. The ROM 1011 stores, for example, a boot program such as a basic input output system (BIOS). The hard disk drive interface 1030 is connected to a hard disk drive 1090. The disk drive interface 1040 is connected to a disk drive 1100. For example, a removable storage medium such as a magnetic disk or an optical disc is inserted into the disk drive 1100. The serial port interface 1050 is connected to, for example, a mouse 1110 and a keyboard 1120. The video adapter 1060 is connected with, for example, a display 1130.

[0108] The hard disk drive 1090 stores, for example, an OS 1091, an application program 1092, a program module 1093, and program data 1094. That is, a program that defines each process executed by the analysis server 10 is implemented as the program module 1093 in which a computer executable code is described. The program module 1093 is stored in, for example, the hard disk drive 1090. For example, the program module 1093 for executing processes similar to those of the functional configuration in the analysis server 10 is stored in the hard disk drive 1090. The hard disk drive 1090 may be replaced with a solid state drive (SSD).

[0109] Data to be used in the processes of the above embodiment is stored in, for example, the memory 1010 or the hard disk drive 1090 as the program data 1094. The CPU 1020 reads the program module 1093 or the program data 1094 stored in the memory 1010 or the hard disk drive 1090 to the RAM 1012 as necessary and executes the program module 1093 or the program data 1094.

[0110] The program module 1093 or the program data 1094 is not limited to being stored in the hard disk drive 1090, and may be stored in, for example, a removable storage medium and read by the CPU 1020 via the disk drive 1100 or the like. Alternatively, the program module 1093 and the program data 1094 may be stored in another computer connected via a network (local area network (LAN), wide area network (WAN), or the like). The program module 1093 and the program data 1094 may be read by the CPU 1020 from another computer via the network interface 1070.

Reference Signs List

[0111]

1	Analysis system
2(2A, 2B, 2C)	Sensing device
10	Analysis server
11	Communication unit
12	Storage unit
13	Control unit
130	Acquisition unit
131	Estimation unit
132	Allocation unit
133	List creation unit
134	List transmission unit
135	Analysis unit
136	Control processing unit

Claims

1. An analysis apparatus comprising:

an acquisition unit that acquires, from each of communication observation devices that observe communication in a network, observation information of the communication including a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address in the communication;

an estimation unit that estimates a topology of the network on the basis of the acquired observation information;

an allocation unit that allocates the communication observation devices such that any one communication observation device on a path of the communication transmits the observation information of the communication for each piece of communication flowing through the network on

the basis of the estimated topology, an installation position of the communication observation device, and the observation information of the communication acquired from the communication observation device;
a list creation unit that creates, for each of the communication observation devices, a monitoring list indicating communication that is a target for transmission of the observation information from the communication observation device on the basis of a result of the allocation; and
a list transmission unit that transmits the created monitoring list for each of the communication observation devices to each of the communication observation devices.

2. The analysis apparatus according to claim 1, wherein

the estimation unit
estimates the topology of the network including an IP address and a MAC address of an apparatus in the network on the basis of the acquired observation information, and
the analysis apparatus further comprises
an analysis unit that compares a pair of an IP address and a MAC address of the apparatus included in the acquired observation information of the communication with a pair of an IP address and a MAC address of the apparatus included in the estimated topology to detect communication performed by an impersonated apparatus.

3. The analysis apparatus according to claim 2, wherein

the analysis unit further
detects whether or not there is a change in the topology of the network by comparing the estimated topology of the network with a past topology of the network.

4. The analysis apparatus according to claim 3, wherein

in a case where the analysis unit detects that there is a change in the topology of the network, the list creation unit
recreates a monitoring list for each of the communication observation devices on the basis of the estimated topology and the observation information, and
the list transmission unit
transmits the recreated monitoring list for each of the communication observation devices to each of the communication observation devices.

5. The analysis apparatus according to claim 2, wherein

the analysis unit further
specifies a monitoring location insufficient for monitoring each piece of communication in the network on the basis of the estimated topology of the network and information regarding an installation location of the communication observation device in the network, and outputs the specified monitoring location.

6. The analysis apparatus according to claim 1, wherein

in a case where a plurality of communication observation devices are installed in a same subnet in the network,
the estimation unit
estimates a topology of an L2 network in the subnet on the basis of a difference between pieces of observation information acquired from the respective communication observation devices.

7. An analysis method executed by an analysis apparatus, comprising:

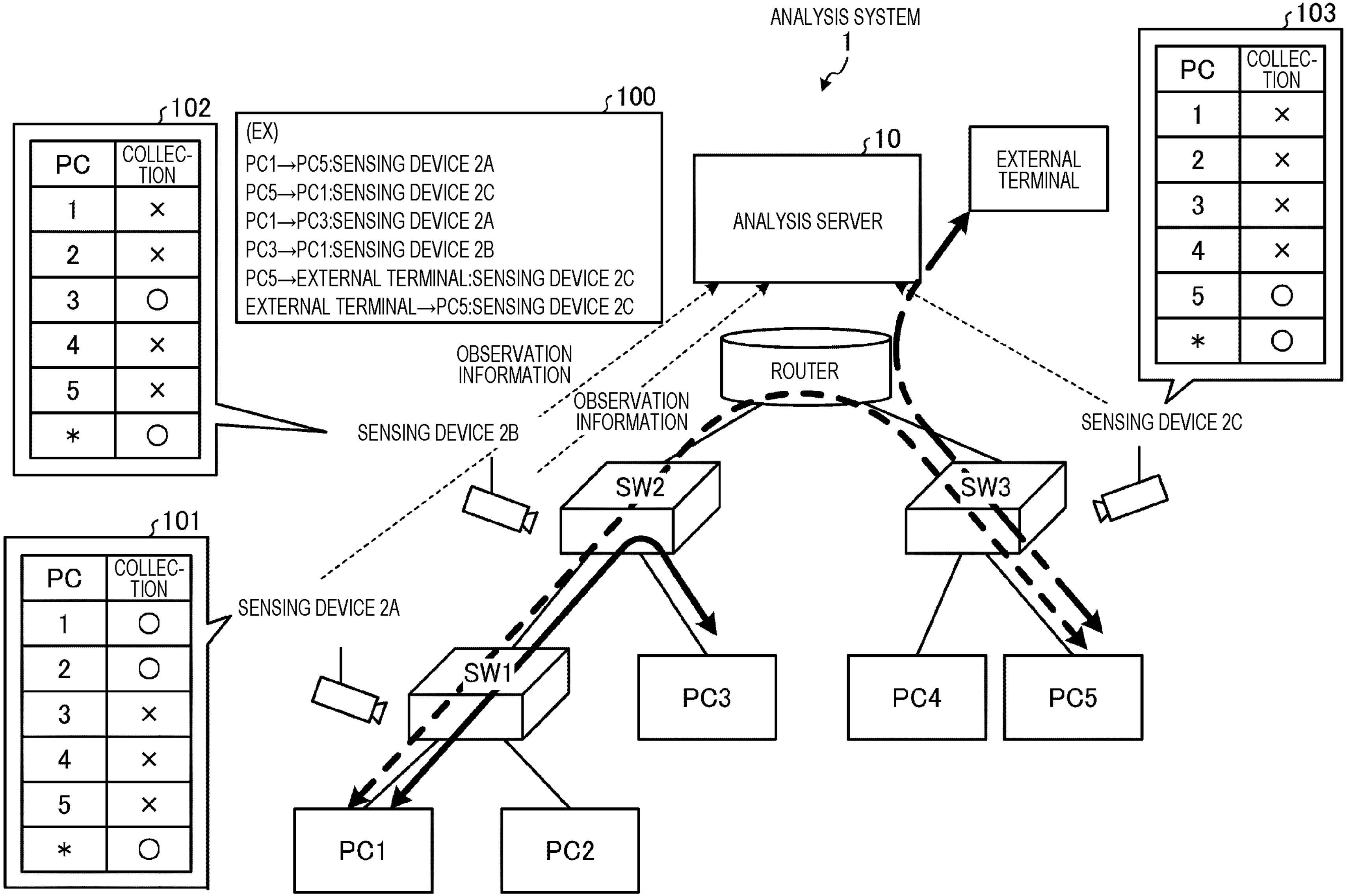
a step of acquiring, from each of communication observation devices that observe communication in a network, observation information of the communication including a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address in the communication;
a step of estimating a topology of the network on the basis of the acquired observation information;
a step of allocating the communication observation devices such that any one communication observation device on a path of the communication transmits the observation information of the communication for each piece of communication flowing through the network on the basis of the estimated topology, an installation position of the communication observation device, and the observation information of the communication acquired from the communication observation device;
a step of creating, for each of the communication observation devices, a monitoring list indicating communication that is a target for transmission of the observation information from the communication observation device on the basis of a result of the allocation; and
a step of transmitting the created monitoring list for each of the communication observation devices to each of the communication observation

devices.

8. An analysis program causing a computer to execute:

a step of acquiring, from each of communication observation devices that observe communication in a network, observation information of the communication including a transmission source IP address, a transmission source MAC address, a transmission destination IP address, and a transmission destination MAC address in the communication;
a step of estimating a topology of the network on the basis of the acquired observation information;
a step of allocating the communication observation devices such that any one communication observation device on a path of the communication transmits the observation information of the communication for each piece of communication flowing through the network on the basis of the estimated topology, an installation position of the communication observation device, and the observation information of the communication acquired from the communication observation device;
a step of creating, for each of the communication observation devices, a monitoring list indicating communication that is a target for transmission of the observation information from the communication observation device on the basis of a result of the allocation; and
a step of transmitting the created monitoring list for each of the communication observation devices to each of the communication observation devices.

Fig. 1



(EX)
PC1→PC5:SENSING DEVICE 2A
PC5→PC1:SENSING DEVICE 2C
PC1→PC3:SENSING DEVICE 2A
PC3→PC1:SENSING DEVICE 2B
PC5→EXTERNAL TERMINAL:SENSING DEVICE 2C
EXTERNAL TERMINAL→PC5:SENSING DEVICE 2C

102

PC	COLLECTION
1	×
2	×
3	○
4	×
5	×
*	○

101

PC	COLLECTION
1	○
2	○
3	×
4	×
5	×
*	○

103

PC	COLLECTION
1	×
2	×
3	×
4	×
5	○
*	○

Fig. 2

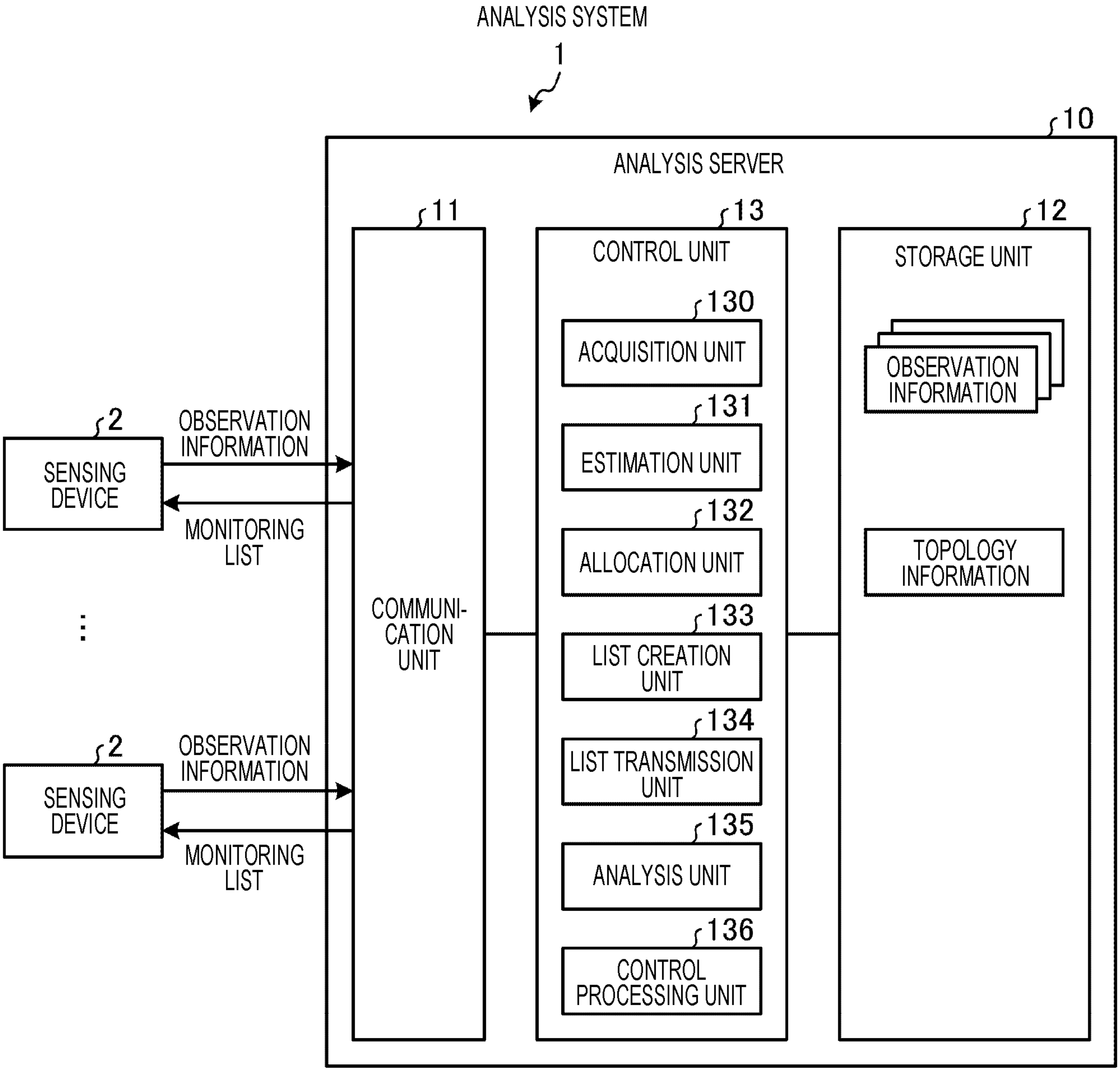
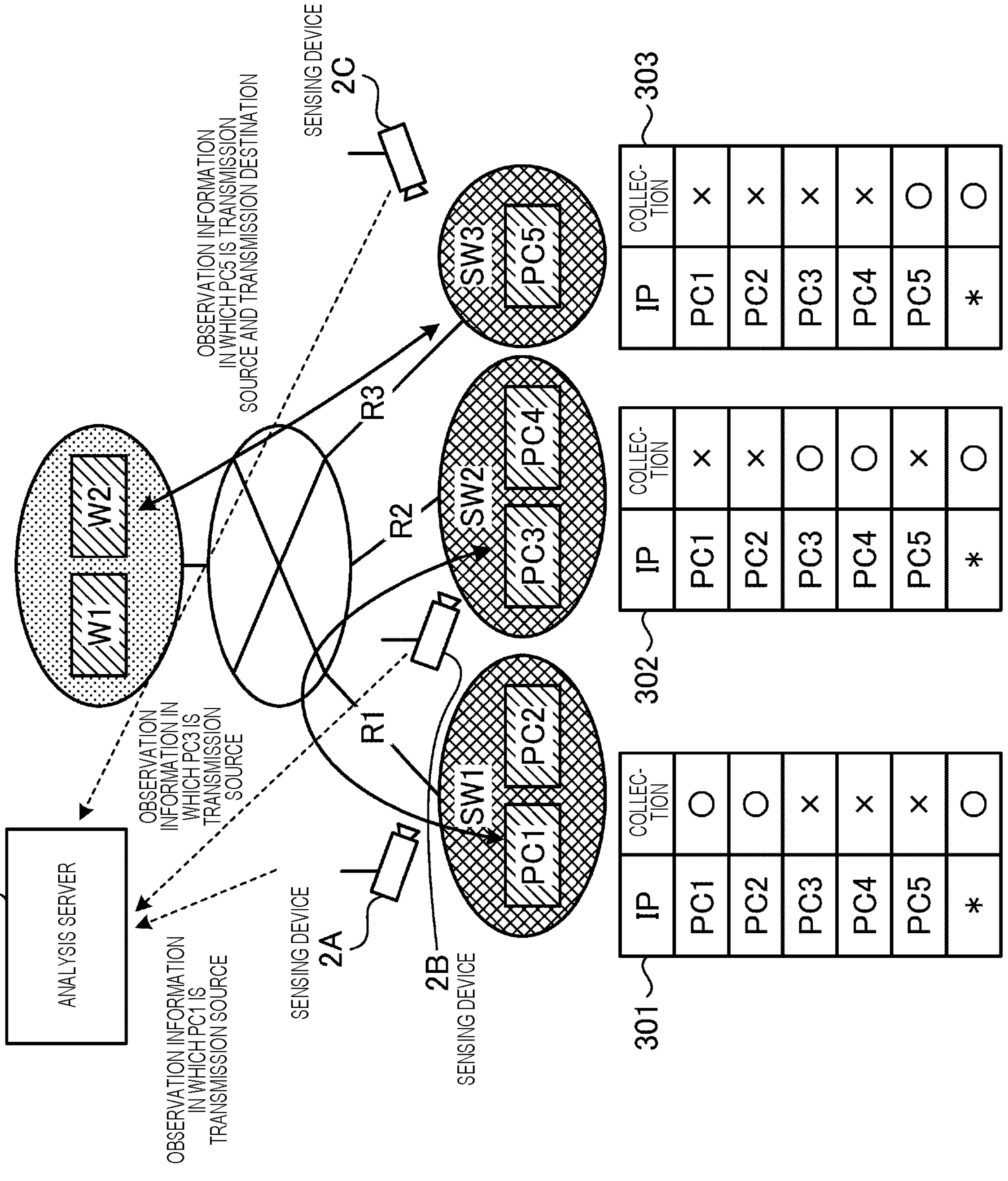

ANALYSIS SYSTEM
1
10
ANALYSIS SERVER
11
13
12
CONTROL UNIT
STORAGE UNIT
130
ACQUISITION UNIT
OBSERVATION INFORMATION
131
ESTIMATION UNIT
2
OBSERVATION INFORMATION
SENSING DEVICE
MONITORING LIST
132
ALLOCATION UNIT
TOPOLOGY INFORMATION
COMMUNI-CATION UNIT
133
LIST CREATION UNIT
134
LIST TRANSMISSION UNIT
2
OBSERVATION INFORMATION
SENSING DEVICE
MONITORING LIST
135
ANALYSIS UNIT
136
CONTROL PROCESSING UNIT

Fig. 3

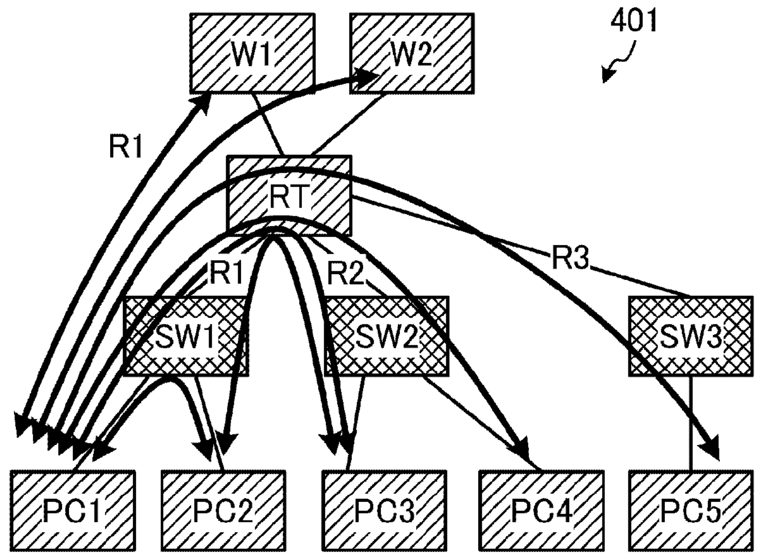

10
ANALYSIS SERVER
W1
W2
OBSERVATION INFORMATION IN WHICH PC1 IS TRANSMISSION SOURCE
OBSERVATION INFORMATION IN WHICH PC3 IS TRANSMISSION SOURCE
OBSERVATION INFORMATION IN WHICH PC5 IS TRANSMISSION SOURCE AND TRANSMISSION DESTINATION
SENSING DEVICE
2A
2B
SENSING DEVICE
SENSING DEVICE
2C
R1
R2
R3
SW1
PC1
PC2
SW2
PC3
PC4
SW3
PC5
301
302
303

IP	COLLEC-TION
PC1	○
PC2	○
PC3	×
PC4	×
PC5	×
*	○

IP	COLLEC-TION
PC1	×
PC2	×
PC3	○
PC4	○
PC5	×
*	○

IP	COLLEC-TION
PC1	×
PC2	×
PC3	×
PC4	×
PC5	○
*	○

Fig. 4



402

ID	Src IP	Src MAC	Dst IP	Dst MAC
SW1	PC1	PC1	PC2	PC2
SW1	PC1	PC1	PC3	*R1*
SW2	PC1	*R2*	PC3	PC3
SW1	PC1	PC1	PC4	*R1*
SW2	PC1	*R2*	PC4	PC4
SW1	PC2	PC2	PC3	*R1*
SW2	PC2	*R2*	PC3	PC3
SW1	PC1	PC1	PC5	*R1*
SW3	PC1	*R3*	PC5	PC5
SW1	PC1	PC1	W1	*R1*
SW1	PC1	PC1	W2	*R1*

403

MAC	IP
PC1	PC1
PC2	PC2
PC3	PC3
PC4	PC4
PC5	PC5
R1	*PC3,PC4,PC5,W1,W2*
R2	*PC1,PC2*
R3	PC1

Fig. 5

402

ID	Src IP	Src MAC	Dst IP	Dst MAC
SW1	PC1	PC1	PC2	PC2
SW1	PC1	PC1	PC3	*R1*
SW2	PC1	*R2*	PC3	PC3
SW1	PC1	PC1	PC4	*R1*
SW2	PC1	*R2*	PC4	PC4
SW1	PC2	PC2	PC3	*R1*
SW2	PC2	*R2*	PC3	PC3
SW1	PC1	PC1	PC5	*R1*
SW3	PC1	*R3*	PC5	PC5
SW1	PC1	PC1	W1	*R1*
SW1	PC1	PC1	W2	*R1*

501

IP Pair	MAC Pair
(PC1,PC3)	(PC1,*R1*),(*R2*,PC3)
(PC1,PC5)	(PC1,*R1*),(*R3*,PC5) (1)
(PC1,W1)	(PC1,*R1*) (2)
(PC1,W2)	(PC1,*R1*) (2)
(PC1,PC3)	(PC1,*R1*),(*R2*,PC5)

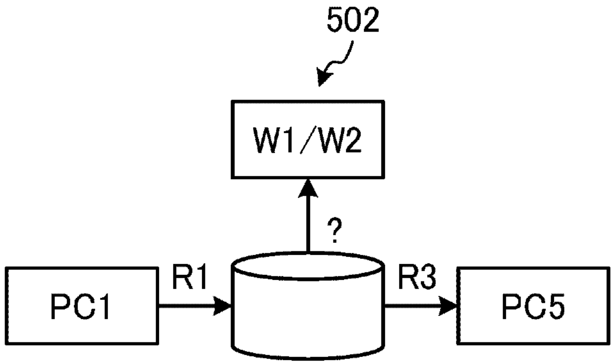


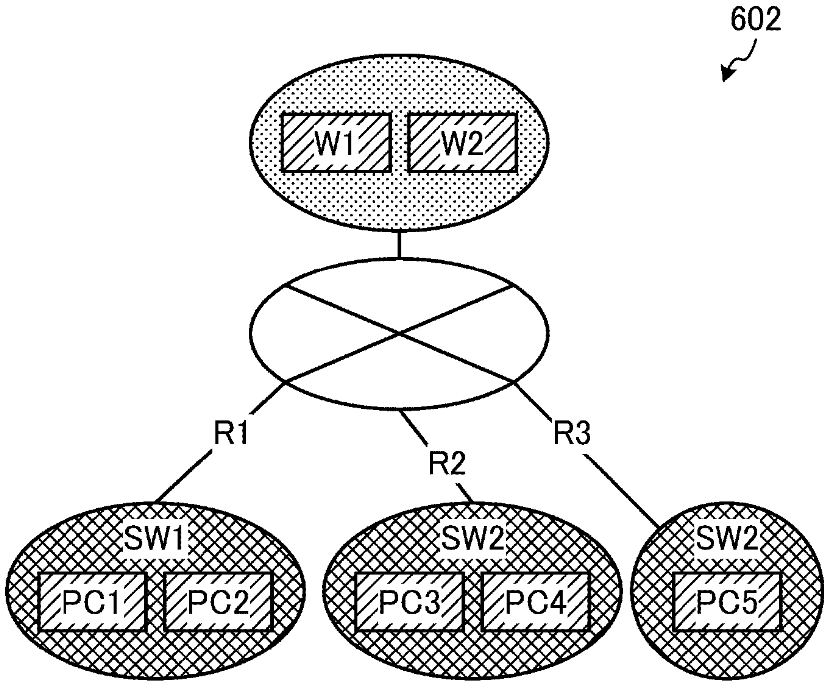
Fig. 6

601

ID	Src IP	Src MAC	Dst IP	Dst MAC
SW1	PC1	PC1	PC2	PC2
SW1	PC1	PC1	PC3	R1
SW2	PC1	R2	PC3	PC3
SW1	PC1	PC1	PC4	R1
SW2	PC1	R2	PC4	PC4
SW1	PC2	PC2	PC3	R1
SW2	PC2	R2	PC3	PC3
SW1	PC1	PC1	PC5	R1
SW3	PC1	R3	PC5	PC5
SW1	PC1	PC1	W1	R1
SW1	PC1	PC1	W2	R1

◯ ··· MAC ADDRESS OF ROUTER

◌ ··· IP ADDRESS OF EXTERNAL TERMINAL



603

IP	COLLEC-TION
PC1	○
PC2	○
PC3	×
PC4	×
PC5	×
*	○

604

IP	COLLEC-TION
PC1	×
PC2	×
PC3	○
PC4	○
PC5	×
*	○

605

IP	COLLEC-TION
PC1	×
PC2	×
PC3	×
PC4	×
PC5	○
*	○

Fig. 7

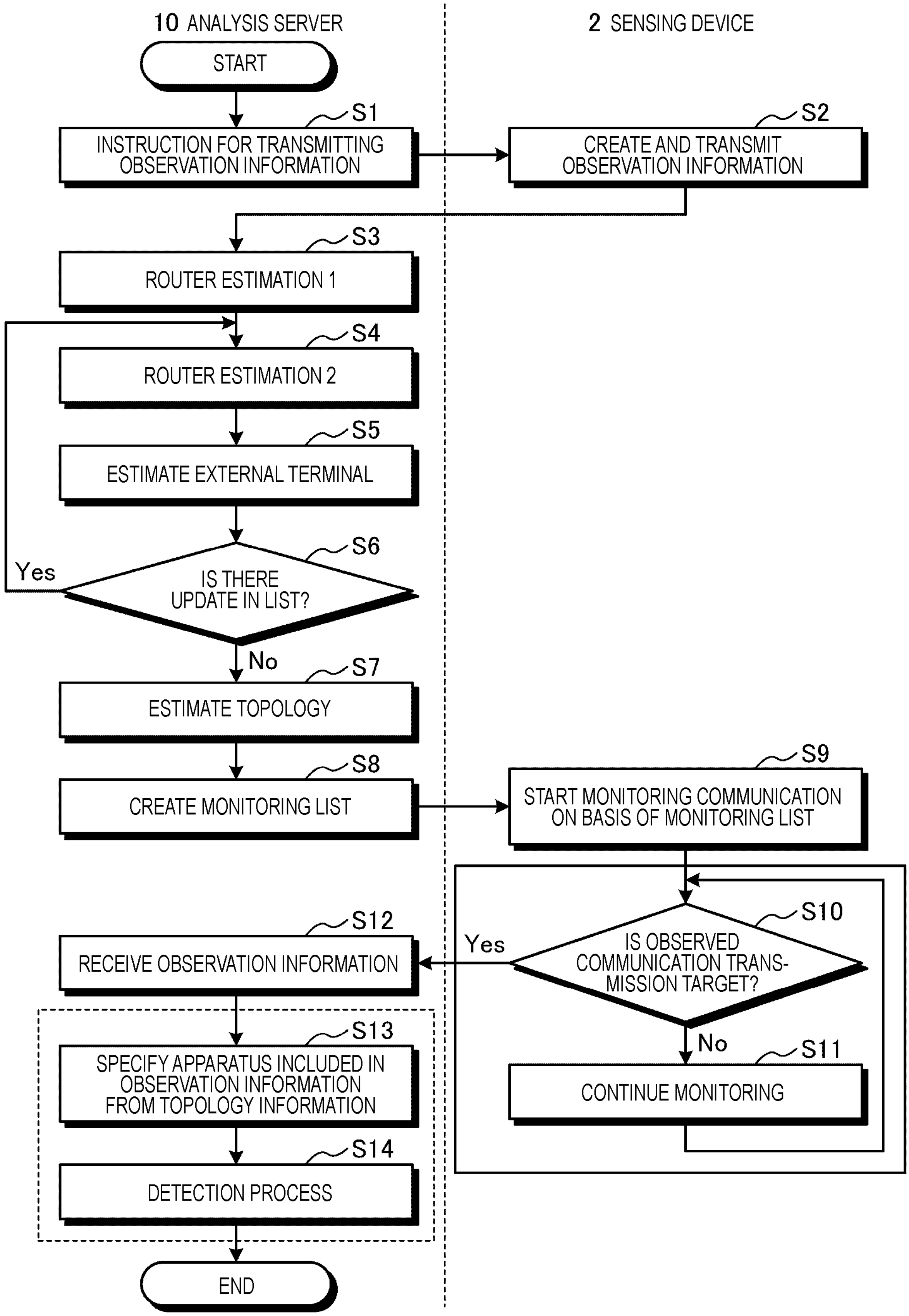

10 ANALYSIS SERVER
2 SENSING DEVICE
START
S1
INSTRUCTION FOR TRANSMITTING OBSERVATION INFORMATION
S2
CREATE AND TRANSMIT OBSERVATION INFORMATION
S3
ROUTER ESTIMATION 1
S4
ROUTER ESTIMATION 2
S5
ESTIMATE EXTERNAL TERMINAL
S6
IS THERE UPDATE IN LIST?
Yes
No
S7
ESTIMATE TOPOLOGY
S8
CREATE MONITORING LIST
S9
START MONITORING COMMUNICATION ON BASIS OF MONITORING LIST
S10
IS OBSERVED COMMUNICATION TRANS-MISSION TARGET?
Yes
No
S11
CONTINUE MONITORING
S12
RECEIVE OBSERVATION INFORMATION
S13
SPECIFY APPARATUS INCLUDED IN OBSERVATION INFORMATION FROM TOPOLOGY INFORMATION
S14
DETECTION PROCESS
END

Fig. 8

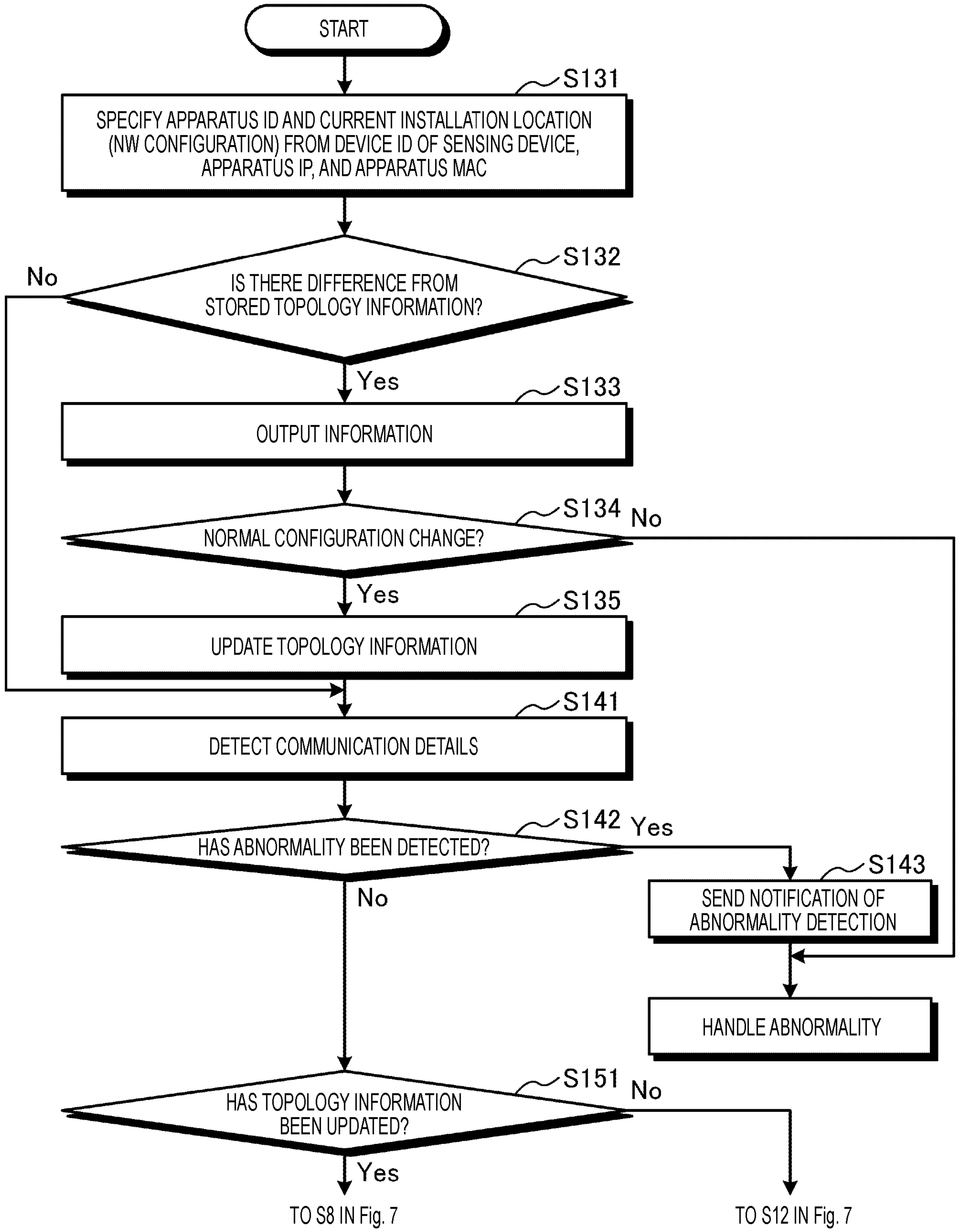

START
S131
SPECIFY APPARATUS ID AND CURRENT INSTALLATION LOCATION (NW CONFIGURATION) FROM DEVICE ID OF SENSING DEVICE, APPARATUS IP, AND APPARATUS MAC
S132
IS THERE DIFFERENCE FROM STORED TOPOLOGY INFORMATION?
No
Yes
S133
OUTPUT INFORMATION
S134
NORMAL CONFIGURATION CHANGE?
No
Yes
S135
UPDATE TOPOLOGY INFORMATION
S141
DETECT COMMUNICATION DETAILS
S142
HAS ABNORMALITY BEEN DETECTED?
Yes
No
S143
SEND NOTIFICATION OF ABNORMALITY DETECTION
HANDLE ABNORMALITY
S151
HAS TOPOLOGY INFORMATION BEEN UPDATED?
No
Yes
TO S8 IN Fig. 7
TO S12 IN Fig. 7

Fig. 9

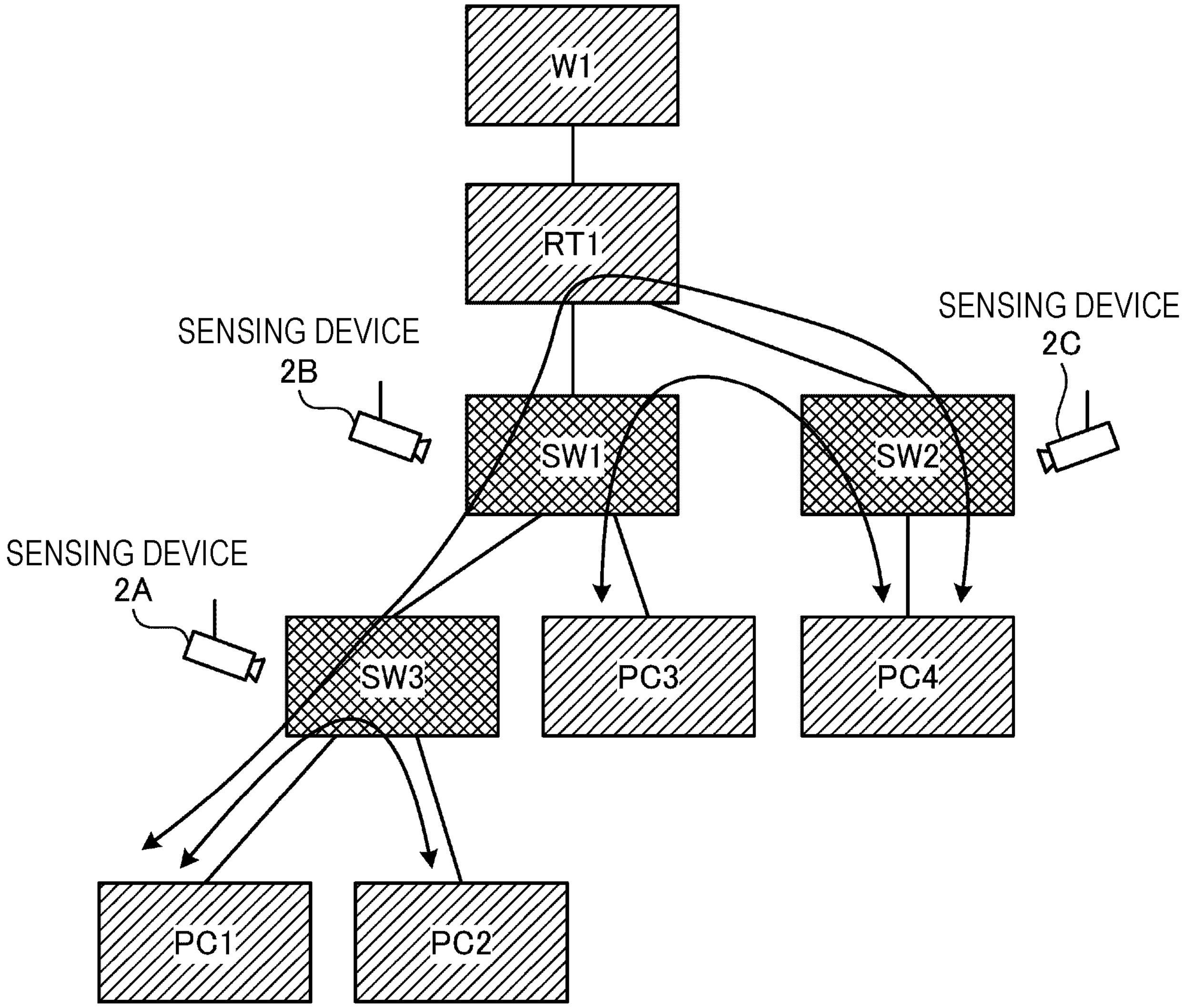

W1
RT1
SENSING DEVICE
2B
SENSING DEVICE
2C
SW1
SW2
SENSING DEVICE
2A
SW3
PC3
PC4
PC1
PC2

Fig. 10

1001

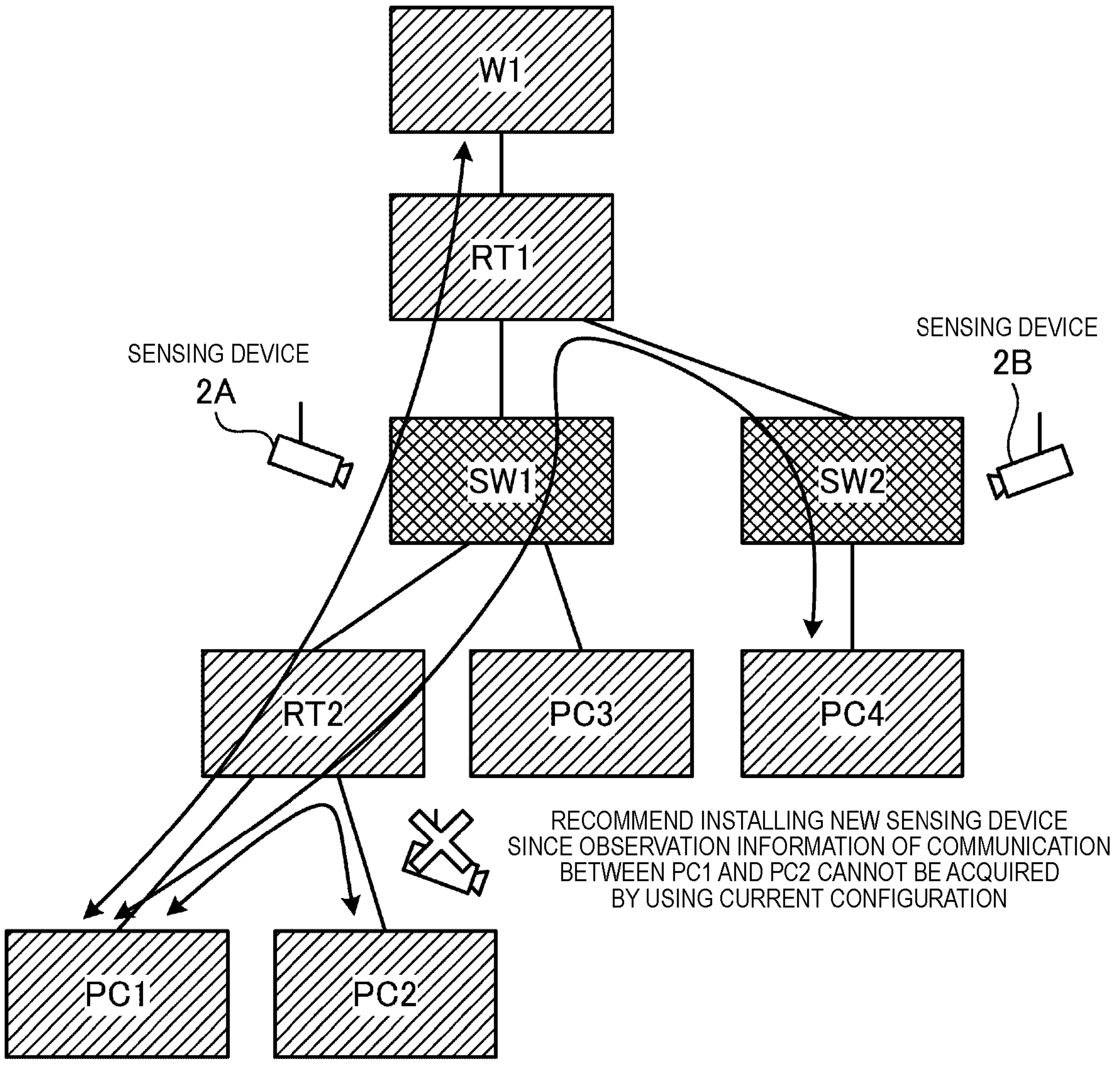
MONITORING LIST FOR SENSING DEVICE 2A

IP	COLLEC-TION
PC1	○
PC2	○
PC3	○
PC4	×
*	○

1002

MONITORING LIST FOR SENSING DEVICE 2B

IP	COLLEC-TION
PC1	×
PC2	×
PC3	×
PC4	○
*	○



RECOMMEND INSTALLING NEW SENSING DEVICE SINCE OBSERVATION INFORMATION OF COMMUNICATION BETWEEN PC1 AND PC2 CANNOT BE ACQUIRED BY USING CURRENT CONFIGURATION

Fig. 11

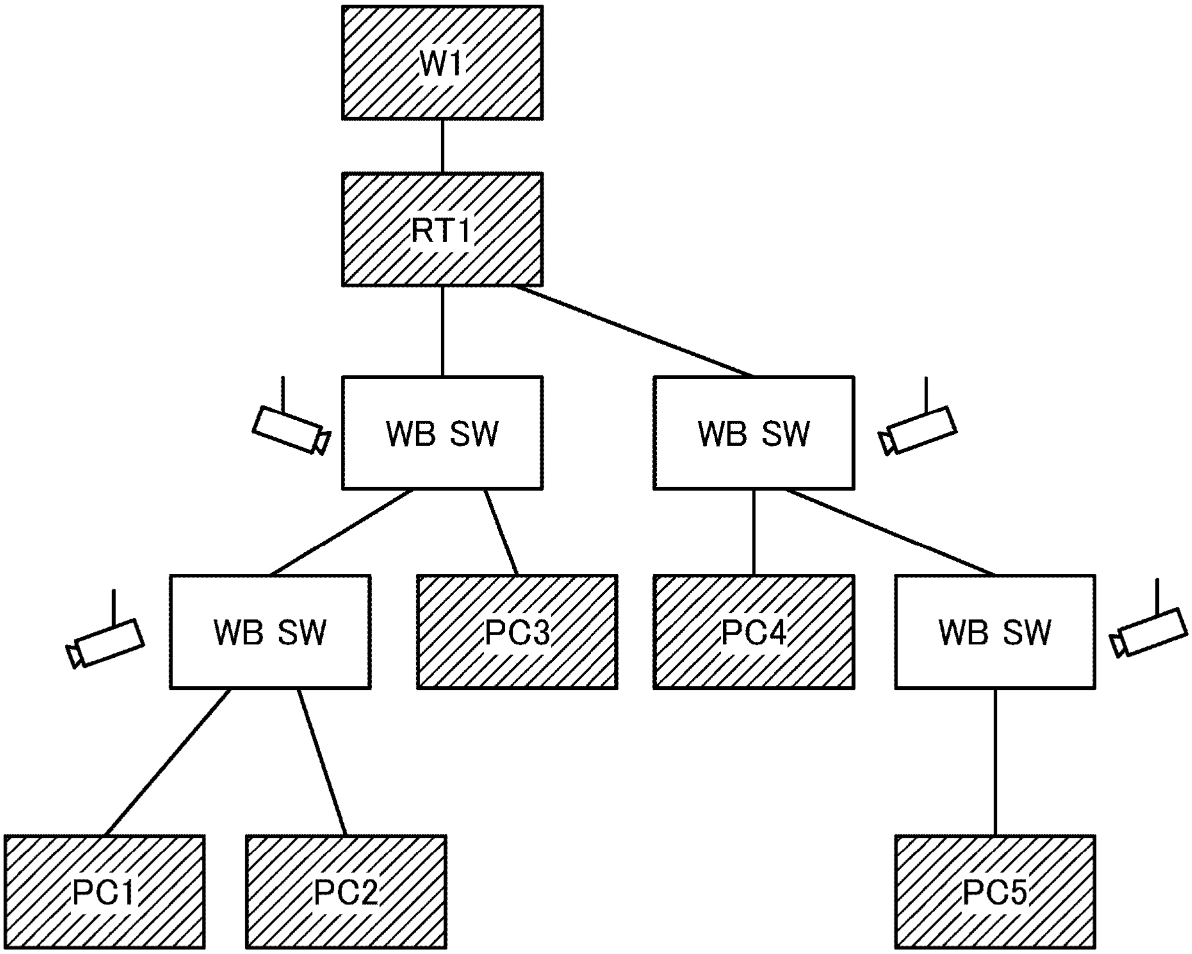
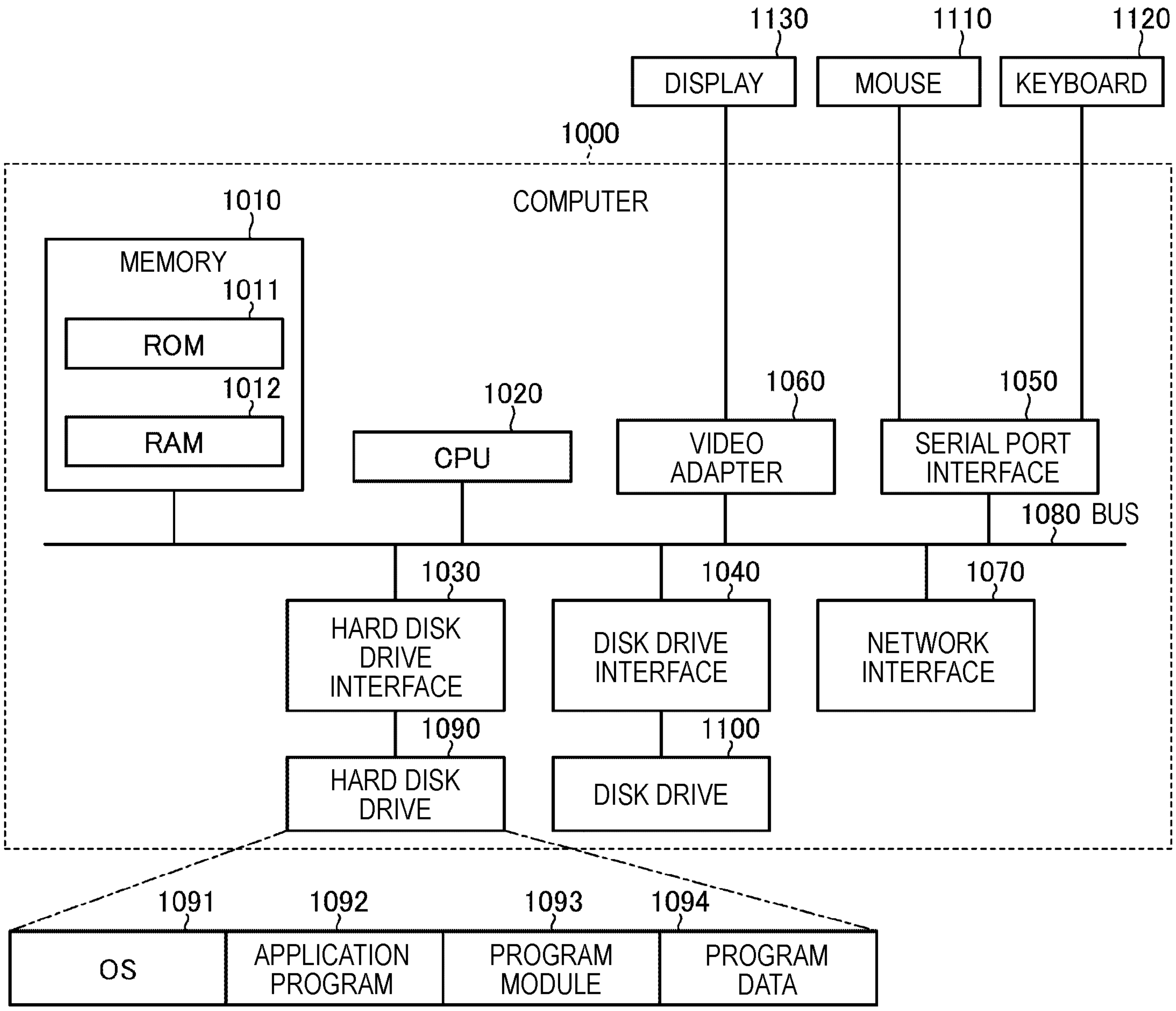


Fig. 12


1130
DISPLAY
1110
MOUSE
1120
KEYBOARD
1000
COMPUTER
1010
MEMORY
1011
ROM
1012
RAM
1020
CPU
1060
VIDEO ADAPTER
1050
SERIAL PORT INTERFACE
1080 BUS
1030
HARD DISK DRIVE INTERFACE
1040
DISK DRIVE INTERFACE
1070
NETWORK INTERFACE
1090
HARD DISK DRIVE
1100
DISK DRIVE
1091
OS
1092
APPLICATION PROGRAM
1093
PROGRAM MODULE
1094
PROGRAM DATA

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/021635

A. CLASSIFICATION OF SUBJECT MATTER
H04L 12/70(2013.01)i
FI: H04L12/70 100Z

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2012/104981 A1 (FUJITSU LIMITED) 09 August 2012 (2012-08–09) entire text, all drawings	1-8
A	JP 2020-77912 A (FUJITSU LTD) 21 May 2020 (2020-05-21) entire text, all drawings	1-8

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 07 July 2021 (07.07.2021)	Date of mailing of the international search report 17 August 2021 (17.08.2021)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/021635

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2012/104981 A1	09 Aug. 2012	US 2013/0297820 A1 entire text, all drawings	
JP 2020-77912 A	21 May 2020	(Family: none)	

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 4809880 B **[0003]**